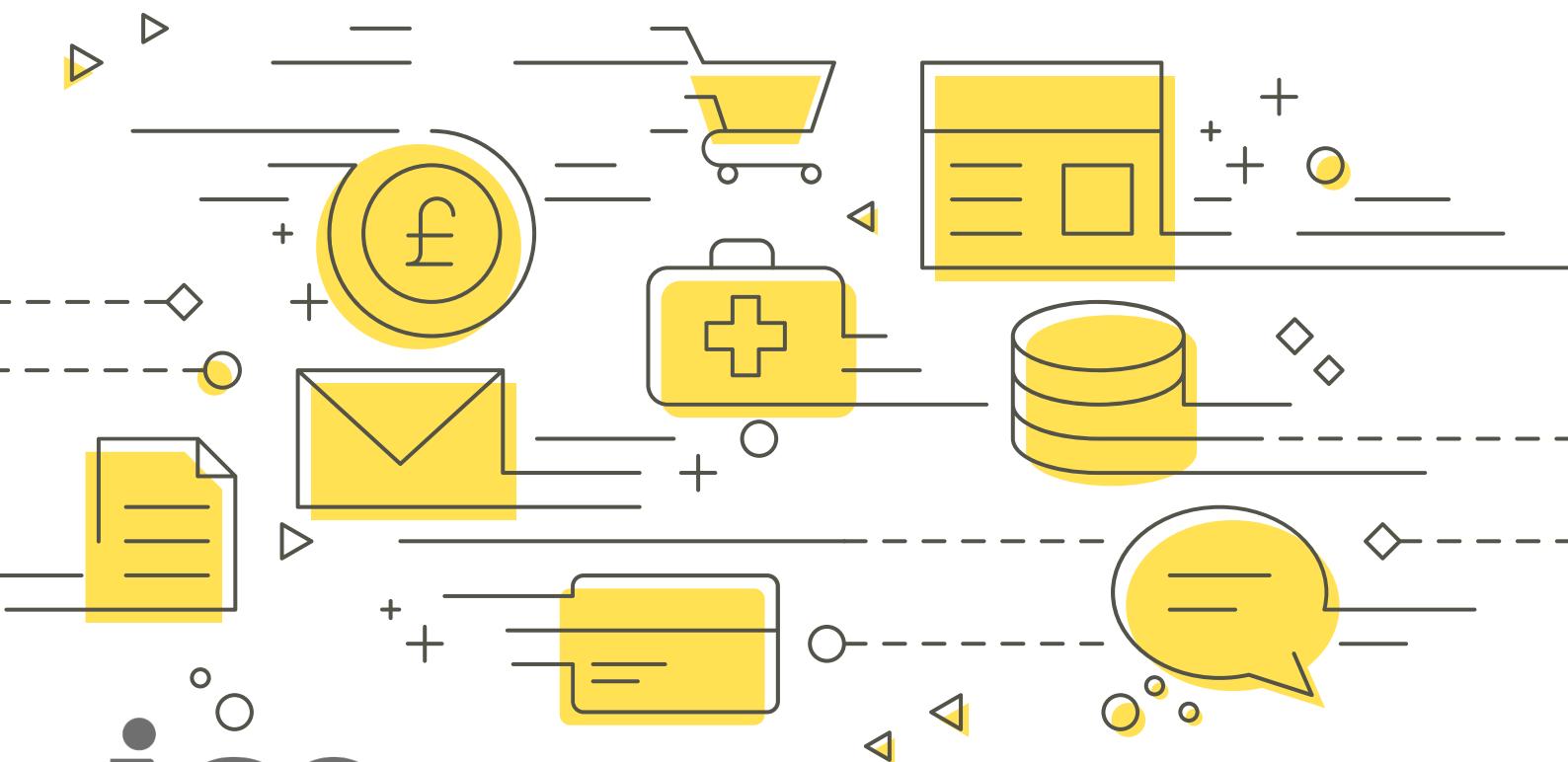


# Draft International data transfer agreement

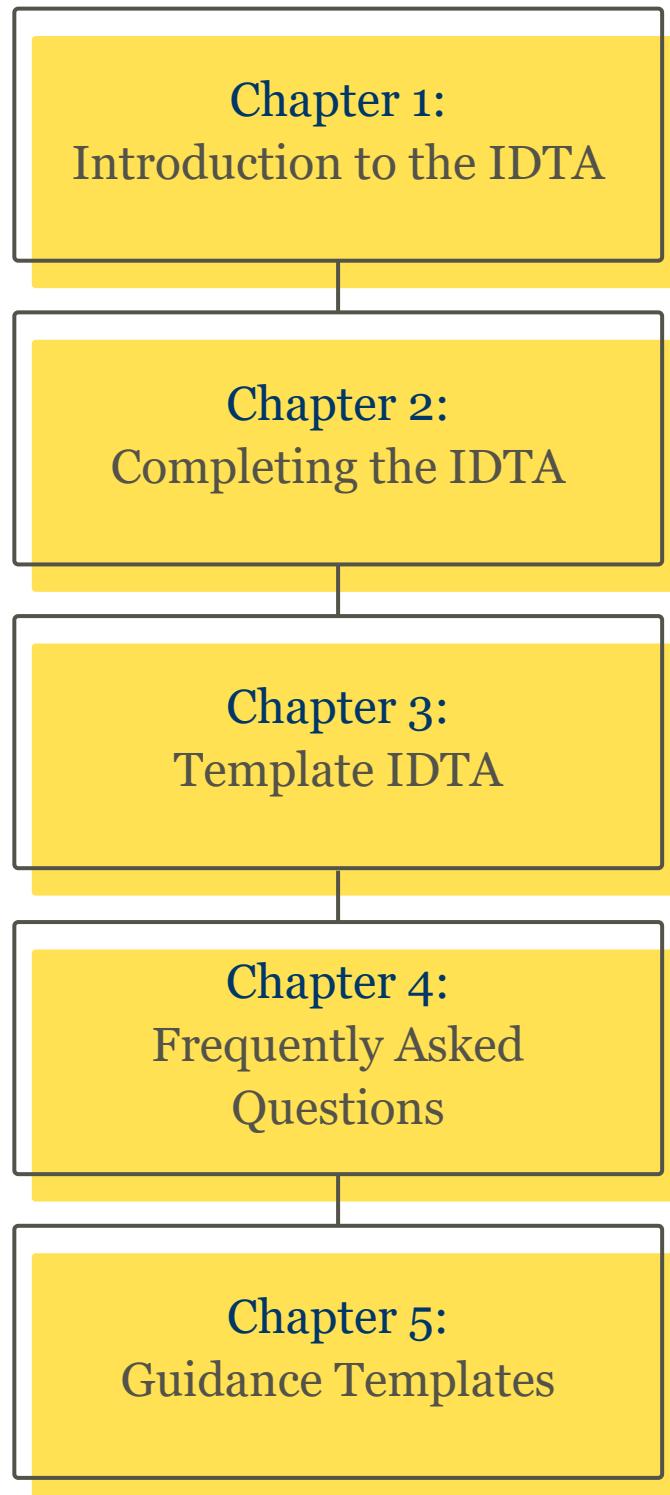
August 2021



**ico.**

Information Commissioner's Office

# Overview



# Contents

<b>Chapter 1: Introduction to the international data transfer agreement (IDTA).....</b>	<b>4</b>
What is the IDTA?.....	4
What is a Restricted Transfer?.....	4
What is a Transfer Risk Assessment? .....	5
How does the IDTA work? .....	5
How does the IDTA link to the other agreements I have with the Importer?.....	5
<b>Chapter 2: Completing the IDTA.....</b>	<b>7</b>
Which data transfers can be used with the IDTA?.....	7
What do I need to do to put the IDTA into place? .....	8
Can I change the format of the IDTA? .....	10
Can more than two parties enter into the IDTA?.....	10
<b>Chapter 3: Template IDTA .....</b>	<b>12</b>
Part one: Tables .....	12
Part two: Extra Protection Clauses .....	20
Part three: Commercial Clauses.....	21
Part four: Mandatory Clauses .....	22
<b>Chapter 4: Frequently Asked Questions.....</b>	<b>56</b>
How do I complete Table 1: Parties and Signature? .....	56
How do I complete Table 2: Transfer Details? .....	57
How do I complete Table 3: Transferred Data? .....	60
How do we complete Table 4: Security Requirements?.....	62
How do we complete Part two: Extra Protection Clauses? .....	63
How do we complete Part three: Commercial Clauses? .....	64
Understanding the Mandatory Clauses .....	64
<b>Chapter 5: Guidance Templates .....</b>	<b>66</b>

# Chapter 1: Introduction to the international data transfer agreement (IDTA)

---

This chapter contains guidance on what the IDTA is and how you can use it to make restricted transfers.

We explain some of the technical data protection terms we use in a Legal Glossary at the end of the third chapter.

## What is the IDTA?

The IDTA is a contract for you to use when making a restricted transfer of personal data to a country outside the UK. We refer to this as the Transferred Data.

The Information Commissioner decided that, the IDTA contains appropriate safeguards for the Transferred Data, including effective and enforceable data subject rights.

The IDTA ensures that the relevant protections for Data Subjects of the Transferred Data, are sufficiently similar to UK protections.

## What is a Restricted Transfer?

We define data transfers as restricted if:

- the UK GDPR applies to the personal data you are transferring;
- you are sending data to or making it accessible by a receiver [to whom the UK GDPR does not apply] OR [located in a country outside the UK]; and
- the receiver is a separate company or individual (including another company in the same corporate group).<sup>1</sup>

Under the UK GDPR, you cannot make a restricted transfer unless:

- it is to a country covered by [UK adequacy regulations](#);
- an exception covers the transfer; or

you make it with appropriate safeguards. An IDTA is one of the UK GDPR's appropriate safeguards.

---

<sup>1</sup> This section will need to be updated following the Consultation: Section 1: Proposal and plans for the ICO to update its guidance on international transfers.

## What is a Transfer Risk Assessment?

You must also complete a transfer risk assessment (TRA) to make sure that the IDTA works as you intend in the country where the receiver of the Personal Data is located.

The TRA checks that local laws and practices do not override the protections that the IDTA contains. This ensures that the relevant protections for Data Subjects of the Transferred Data are sufficiently similar to the UK's protections. ICO's guidance on TRAs may evolve over time relating to changes in legislation, caselaw and practical review of the operation of the guidance.

## How does the IDTA work?

You, the person sending the data, are the Exporter. The person who receives the data is the Importer. The Exporter and the Importer both enter into the IDTA.

The IDTA contains:

- tables which you should use to set out specific information about the Exporter, the Importer and the restricted transfer;
- the option to include extra protection clauses. When you complete your TRA, you may decide that the IDTA needs extra steps in order to provide the right level of protection. These can be set out in this section, but must be included in the IDTA or the Linked Agreement if the IDTA is to work as an appropriate safeguard;
- the option to include commercial clauses agreed by the Exporter and Importer, provided that these do not contradict the IDTA; and
- a set of Mandatory Clauses which must always be included. This includes the Legal Glossary.

## How does the IDTA link to the other agreements I have with the Importer?

When you make a restricted transfer, you will often, but not always, also have a service, data sharing or processing agreement between you and the Importer.

In particular, if the Importer is your Processor or Sub-Processor, the UK GDPR requires you to have an agreement in place. The agreement must contain specific terms, as Article 28 UK GDPR requires.

We call these 'Linked Agreements' in the IDTA, as they link to the restricted transfer you are making. They are useful as they often contain a lot of the information you need to complete the tables. In those cases, you can refer to the relevant section of the Linked Agreement.

It is very important that, if any of the terms contradict each other, the IDTA terms override the Linked Agreements. This is to make sure that the Transferred Data has the right level of protection set out in the IDTA.

## Chapter 2: Completing the IDTA

This chapter contains guidance on how to use the IDTA.

We explain some of the technical data protection terms we use in a Legal Glossary at the end of the third chapter.

### Which data transfers can be used with the IDTA?

The IDTA is designed to be used for the following information flows:<sup>2</sup>

Transfers from:	Transfers to
Sender/Exporter:  In each case, its Processing of the Transferred Data is governed by UK GDPR, and may be located in the UK or outside the UK	Receiver/Importer:  In each case it is a separate legal person or organisation to the sender/exporter
Controller or Joint Controller	Any party which is not its Processor for example another Controller  [to which the UK GDPR does not apply] OR [located in a country outside the UK]
Controller or Joint Controller	Its Processor  [to which the UK GDPR does not apply] OR [located in a country outside the UK]
Processor	Its Sub-Processor  [to which the UK GDPR does not apply] OR [located in a country outside the UK]
Processor (with a UK GDPR Controller)	Any party which is not its Controller or Sub-Processor  [to which the UK GDPR does not apply] OR [located in a country outside the UK]

<sup>2</sup> This table will need to be updated following the Consultation: Section 1: Proposal and plans for the ICO to update its guidance on international transfers

Sub-Processor	Its Sub-Sub-Processor [to which the UK GDPR does not apply] OR [located in a country outside the UK]
Sub-Processor (with a UK GDPR Controller)	Any party which is not its Controller or Processor [to which the UK GDPR does not apply] OR [located in a country outside the UK]

It is not a restricted transfer (and so the IDTA does not cover this) where you are a Processor, and your Processing is subject to UK GDPR, but your Controller is not subject to UK GDPR. The only exception is if you are sending data to your Sub-Processor [to which the UK GDPR does not apply] OR [located in a country outside the UK]; this is a restricted transfer, and so is covered by the IDTA.<sup>3</sup>

## What do I need to do to put the IDTA into place?

First you need to complete your transfer risk assessment (TRA). Once this is complete and you are satisfied with the protections (including any Security Requirements and Extra Protection Clauses), you can put the IDTA into place.

The IDTA itself is divided into four parts. The table below sets out what you need to do for each part of the IDTA.

Chapter 4 sets out FAQs with more detailed guidance on how to complete the IDTA and what it means.

Part	What you need to do
Part one: Tables  Table 1: Parties and signature  Table 2: Transfer Details  Table 3: Transferred Data  Table 4: Security Requirements	Complete with details about the specific information about the Parties and the restricted transfer.  We provide template tables, but you do not need to use them.  Just make sure you include all the relevant information in your IDTA (including those selections we provide as tick boxes) and your cross-references are correct.  Both parties need to sign the contract in Table 1 in order for the IDTA to be in force.

<sup>3</sup> This section will need to be updated following the Consultation: Section 1: Proposal and plans for the ICO to update its guidance on international transfers.

	<p>There are other ways to enter into a contract, but signing is the simplest way to evidence that the parties agree to be bound by the IDTA. You can use other methods if you choose, provided that the IDTA is binding on the parties.</p>
Part two: Extra Protection Clauses	<p>If your TRA identifies that you need extra steps and protections to protect the Transferred Data, you must add in clauses setting these out here.</p> <p>If you prefer, you include some or all of those clauses in Table 4: Security requirements instead. It can be helpful to insert them here so you can easily identify them when you review the TRA, but this is not a requirement.</p> <p>We provide a template format, but you do not need to use it. Just make sure that the Mandatory Clauses correctly cross-refer to these Extra Protection Clauses.</p>
Part three: Commercial Clauses	<p>This is the section where you can include agreed commercial clauses.</p> <p>We provide a template format, but you do not need to use it.</p> <p>For example, you may not need to add any commercial clauses if you have a Linked Agreement.</p> <p>If you are not using any Commercial Clauses, the simplest thing to do is to state "Commercial Clauses are not used" in this section. Another option is to remove all the references to the Commercial Clauses in the Mandatory Clauses.</p> <p>You must be cautious when adding in commercial clauses. Your restricted transfer may breach UK GDPR if you inadvertently reduce the level of protection in the IDTA.</p>
Part four: Mandatory Clauses	<p>Include these clauses <b>in full and without any changes</b> in every IDTA.</p> <p>The only exceptions are if you:</p> <ul style="list-style-type: none"> <li>• do not use the same format for Parts one, two and three, you may change the words in the Mandatory Clauses to cross-reference to the</li> </ul>

	<p>information contained in those parts; or</p> <ul style="list-style-type: none"> <li>• you remove those sections which expressly do not apply to the parties;</li> <li>• have more than two parties to the IDTA, you may make changes so that it operates as a multi-party contract.</li> </ul> <p>You must be cautious when making these changes. Your restricted transfer may breach UK GDPR if you inadvertently reduce the level of protection in the IDTA.</p>
--	---

## Can I change the format of the IDTA?

Yes.

If you are not using the Tables in Parts one, two and three, you may change the cross-references in the Mandatory Clauses to the headings and locations you are using. This should only be so that the IDTA works as you intend using your format.

You may also to remove those Sections of the IDTA which are expressly stated not to apply to the selections you have made in Table 2: Transfer Details, that you or the other Party is a Controller, Processor or Sub-Processor and/or that the Importer is subject to, or not subject to, the UK GDPR.

Be cautious when making any changes to the Mandatory Clauses. Your restricted transfer may be in breach of UK GDPR if you inadvertently reduce the level of protection of the IDTA. You may want to seek professional advice.

The IDTA does not include:

- words in square brackets, which are instructions or guidance; and
- the column headed "Guidance" in the Legal Glossary.

You do not need to, but if you wish you can delete these from your IDTA.

## Can more than two parties enter into the IDTA?

Yes.

In that case you may make changes to the Mandatory Clauses. This should only be so that the IDTA works as you intend, but with more than one Exporter or Importer.

A multi-party IDTA may nominate someone to make decisions on everyone's behalf.

Chapter 5 of this guidance includes a template for multi-parties<sup>4</sup>.

Be cautious when making any changes to the Mandatory Clauses. Your restricted transfer may breach UK GDPR if you inadvertently reduce the level of protection of the IDTA. You may want to seek professional advice.

---

<sup>4</sup> This will be produced once we have finalised the IDTA following the consultation.

## Chapter 3: Template IDTA

[Guidance: Within the Template IDTA are instructions and guidance. They are in square brackets and always start with the word "Instructions:" or "Guidance:" You may delete these sentences. They are not binding and do not form part of the IDTA.]

We define words and phrases which start with a capital letter in the Legal Glossary in Section 37.

In the Instructions and Guidance when we refer to "you" we mean the Exporter.]

This IDTA has been issued by the Information Commissioner for Parties making restricted transfers. The Information Commissioner considers that it provides Appropriate Safeguards for restricted transfers when it is entered into as a legally binding contract.

### Part one: Tables

[Instructions: We provide a template format, but you do not need to use it. Just make sure that you provide all the information set out in the table below and that the Mandatory Clauses correctly cross-refer to this information.]

**Table 1: Parties and signatures**

<b>Start Date</b>	[Instructions: Insert start date of IDTA. If the parties agree, the start date can be either before or after both have signed.]	
<b>The Parties</b>	<b>Exporter (who sends the restricted transfer)</b>	<b>Importer (who receives the restricted transfer)</b>
<b>Parties' details</b>	Full legal name: Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier):

<b>Key Contact</b>	Full Name (optional): Job Title: [REDACTED] Contact details including email: [REDACTED]	Full Name (optional): Job Title: [REDACTED] Contact details including email: [REDACTED]
<b>Importer Data Subject Contact</b>		Job Title: [REDACTED] Contact details including email: [REDACTED]
<b>Signatures confirming each Party agrees to be bound by this IDTA</b>	Signed for and on behalf of the <b>Exporter</b> set out above Signed: [REDACTED] Date of signature: [REDACTED] Full name: [REDACTED] Job title: [REDACTED]	Signed for and on behalf of the <b>Importer</b> set out above Signed: [REDACTED] Date of signature: [REDACTED] Full name: [REDACTED] Job title: [REDACTED]

**Table 2: Transfer Details**

<b>UK country's law that governs the IDTA:</b>	[Instructions: Select which country's law applies to this IDTA. You can only choose one:] <input type="checkbox"/> England & Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
<b>Place for legal claims to be made</b>	[Instructions: Select in which country's courts you can bring a legal claim. You can select more than one:] <input type="checkbox"/> England and Wales <input type="checkbox"/> Northern Ireland <input type="checkbox"/> Scotland
<b>The status of</b>	[Instructions: Select one option:] In relation to the Processing of the Transferred Data: <input type="checkbox"/> Importer is a Controller

<b>the importer<sup>5</sup></b>	<input type="checkbox"/> Importer is the Exporter's Processor or Sub-Processor <input type="checkbox"/> Importer is <b>not</b> the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
<b>Whether UK GDPR applies to the Importer<sup>6</sup></b>	<p>[Instructions: Select one option:]</p> <input type="checkbox"/> UK GDPR applies to the Importer's Processing of the Transferred Data <input type="checkbox"/> UK GDPR does not apply to the Importer's Processing of the Transferred Data
<b>Linked Agreement<sup>7</sup></b>	<p>[Instructions: If there is more than one Linked Agreement, please number them sequentially below. You should use this number when you refer to that specific Linked Agreement in these Tables.]</p> <p><b>If the Importer is the Exporter's Processor or Sub-Processor</b> – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: [REDACTED]</p> <p>Name of agreement: [REDACTED]</p> <p>Date of agreement: [REDACTED]</p> <p>Parties to the agreement: [REDACTED]</p> <p><b>Other agreements</b> – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: [REDACTED]</p> <p>Name of agreement: [REDACTED]</p> <p>Date of agreement: [REDACTED]</p> <p>Parties to the agreement: [REDACTED]</p> <p><b>If the Exporter is a Processor or Sub-Processor</b> – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: [REDACTED]</p>

<sup>5</sup> This section may need to be updated following the Consultation Section 1: Proposal and plans for the ICO to update its guidance on international transfers

<sup>6</sup> This section may need to be updated following the Consultation Section 1: Proposal and plans for the ICO to update its guidance on international transfers

<sup>7</sup> This section may need to be updated following the Consultation Section 1: Proposal and plans for the ICO to update its guidance on international transfers

	<p>Name of agreement: [REDACTED]</p> <p>Date of agreement: [REDACTED]</p> <p>Parties to the agreement: [REDACTED]</p>
<b>Term</b>	<p>The Importer may Process the Transferred Data for the following time period:</p> <p>[Instructions: Select one option. If you select "Time period", you must add the time period in here.]</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Time period:</li> <li><input type="checkbox"/> the period for which the Linked Agreement is in force</li> <li><input type="checkbox"/> (only if the Importer is a Controller or <u>not</u> the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.</li> </ul>
<b>Ending the IDTA before the end of the Term</b>	<p>[Instructions: Select one option:]</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA.</li> <li><input type="checkbox"/> the Parties can end the IDTA before the end of the Term by serving:</li> </ul> <p>months'</p> <p>written notice, as set out in Section 29 (How to end this IDTA without there being a breach).</p>
<b>Can the Importer make further transfers of the Transferred Data?</b>	<p>[Instructions: Select one option:]</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</li> <li><input type="checkbox"/> The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).</li> </ul> <p>[Guidance: The Importer may always transfer on the data as set out in Section 23 (Direct Access and Access Requests).]</p>

**Specific restrictions when the Importer may transfer on the Transferred Data**

[Instructions: You only need to complete this box if you have ticked that the Importer MAY transfer on the Transferred Data in accordance with Section 16.1 (Transferring on the Transferred Data)]

The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:

[Instructions: Select all the options which apply:]

- if the Exporter tells it in writing that it may do so.
- to: [redacted]

[Instructions: insert a list of the authorised receivers or a list of categories of receivers.]

- to the authorised receivers (or the categories of authorised receivers) set out in:

[Instructions: Insert reference of the Linked Agreement.]

- there are no specific restrictions.

**Review Dates**

[Guidance: if this is a one-off transfer and the Importer does not retain any Transferred Data, you do not need to review the IDTA during the Term. The purpose of the review is to ensure that the IDTA continues to provide Appropriate Safeguards, in particular considering the Importer Information, the Security Requirements and Extra Protection Clauses.]

[Instructions: Either choose no review is needed. Otherwise set out the first review date and then the period when reviews must take place]

- No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data

First review date:

The Parties must review this IDTA at least once each:

- month
- quarter
- 6 months
- year

**Table 3: Transferred Data**

<b>Transferred Data</b>	<p>The personal data to be sent to the Importer under this IDTA consists of:</p> <p>[Instructions: Insert categories of Personal Data or insert Linked Agreement and the relevant clause]</p> <p>[Instructions: Where you have referred to a Linked Agreement select one option:]</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.</li> <li><input type="checkbox"/> The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.2</li> </ul>
<b>Special Categories of Personal Data and criminal convictions and offences</b>	<p>The Transferred Data includes data relating to:</p> <p>[Instructions: Select all which apply:]</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> racial or ethnic origin</li> <li><input type="checkbox"/> political opinions</li> <li><input type="checkbox"/> religious or philosophical beliefs</li> <li><input type="checkbox"/> trade union membership</li> <li><input type="checkbox"/> genetic data</li> <li><input type="checkbox"/> biometric data for the purpose of uniquely identifying a natural person</li> <li><input type="checkbox"/> physical or mental health</li> <li><input type="checkbox"/> sex life or sexual orientation</li> <li><input type="checkbox"/> criminal convictions and offences</li> <li><input type="checkbox"/> none of the above</li> <li><input type="checkbox"/> set out in: [Instructions: Insert reference of the Linked Agreement.]</li> </ul> <p>[Instructions: Where you have referred to a Linked Agreement select one option:]</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The categories of special category and criminal records data will update automatically if the information is</li> </ul>

	<p>updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.2</p>
<p><b>Relevant Individuals</b></p>	<p>The Data Subjects of the Transferred Data are:</p> <p>[Instructions: Insert the categories of Data Subject or insert name of Linked Agreement and the relevant clause]</p> <p>[Instructions: Where you have referred to a Linked Agreement select one option:]</p> <p><input type="checkbox"/> The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The categories of Data Subjects will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.2</p>
<p><b>Purpose</b></p>	<p>[Instructions: You must choose one or both of the options below.]</p> <p><input type="checkbox"/> The Importer may Process the Transferred Data for the following purposes:</p> <p>[Instructions: Set out the purpose or each of the purposes if there is more than one.]</p> <p><input type="checkbox"/> The Importer may Process the Transferred Data for the purposes set out in:</p> <p>[Instructions: insert reference of the Linked Agreement.]</p> <p>In both cases, any other purposes which are compatible with the purposes set out above.</p> <p>[Instructions: Where you have referred to a Linked Agreement select one option:]</p> <p><input type="checkbox"/> The purposes will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.2</p>

**Table 4: Security Requirements:**

<b>Security of Transmission</b>	[Instructions: insert details or insert reference to section of Linked Agreement.]
<b>Security of Storage</b>	[Instructions: insert details or insert reference to section of Linked Agreement.]
<b>Security of Processing</b>	[Instructions: insert details or insert reference to section of Linked Agreement.]
<b>Organisational security measures</b>	[Instructions: insert details or insert reference to section of Linked Agreement.]
<b>Technical security minimum requirements</b>	[Instructions: insert details or insert reference to section of Linked Agreement.]
<b>Updates to the Security Requirements</b>	<p>[Instructions: Where you have referred to a Linked Agreement select one option:]</p> <p><input type="checkbox"/> The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.</p> <p><input type="checkbox"/> The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.2</p>

## Part two: Extra Protection Clauses

[Instructions: We provide a template format, but you do not need to use it. Just make sure that you provide all of the information set out in the table below and that the Mandatory Clauses correctly cross-refer to this information.]

<b>Extra Protection Clauses:</b>	[Instructions: If, having considered the protections available to the Transferred Data and any TRA, you decide that you need extra steps and protections in order to maintain the right level of protection in the IDTA, those extra steps and protections must be set out in clauses in this IDTA. You may add those clauses in here.]
<b>(i) Extra technical security protections</b>	[Instructions: these are additional technical security protections. You may choose to include these in Table 4 Security Requirements. If so, you do not need to set them out here. However, it can be helpful to include them here (or cross refer to them) for when you review the IDTA.]
<b>(ii) Extra organisational protections</b>	[Instructions: these are additional organisational protections. For additional organisational security protections, you may choose to include them in Table 4 Security Requirements. If so, you do not need to set them out here. However, it can be helpful to include them here (or cross refer to them) for when you review the IDTA.]
<b>(iii) Extra contractual protections</b>	[Instructions: these are additional contractual protections. For additional contractual security protections, you may choose to include them in Table 4 Security Requirements. If so, you do not need to set them out here. However, it can be helpful to include them here (or cross refer to them) for when you review the IDTA.]

## Part three: Commercial Clauses

[Instructions: You may add commercial clauses, but you are not required to do so.]

We provide a template format, but you do not need to use it. For example, you may not need to add any Commercial Clauses if you have a Linked Agreement.

If you are not using any Commercial Clauses, the simplest thing to do is to state "Commercial Clauses are not used" in this section.

You must be cautious when adding in commercial clauses. If you inadvertently reduce the level of protection in the IDTA then those commercial clauses will not be enforceable and your restricted transfer may be in breach of UK GDPR.]

### **Commercial Clauses**

[Instructions: Insert additional commercial clauses agreed by the Parties, if any.]

## Part four: Mandatory Clauses<sup>8</sup>

### Information that helps you to understand this IDTA

#### 1. This IDTA and Linked Agreements

- 1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
- 1.2 This IDTA is made up of:
  - 1.2.1 Part one: Tables;
  - 1.2.2 Part two: Extra Protection Clauses;
  - 1.2.3 Part three: Commercial Clauses; and
  - 1.2.4 Part four: Mandatory Clauses.
- 1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
- 1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Parties confirm that there is a Linked Agreement between the Parties which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
- 1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with this IDTA.

#### 2. Legal Meaning of Words

- 2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 37.
- 2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

#### 3. You have provided all the information required

- 3.1 The Parties promise that the information contained in Part one: Tables is correct and complete.

---

<sup>8</sup> Various sections of the IDTA will need to be updated following the Consultation Section 1: Proposal and plans for the ICO to update its guidance on international transfers

- 3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR, is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:
  - 3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and
  - 3.2.2 the Parties and any Relevant Individuals are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.
- 3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong in law, then the terms and conditions of the IDTA will still apply to the greatest extent possible.

#### **4. How to sign the IDTA**

- 4.1 The Parties may choose to each sign (or execute):
  - 4.1.1 the same copy of this IDTA;
  - 4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;
  - 4.1.3 a separate, identical copy. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

#### **5. Changing this IDTA**

- 5.1 Each Party must not change the Mandatory Clauses, except only:
  - 5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information;
  - 5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR (acknowledging that the removed sections may still apply if the wrong selection is made); and/or

- 5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses),

provided that the changes do not reduce the Appropriate Safeguards.

- 5.2 If the Parties wish to change Part one, Part two or Part three, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

## 6. Understanding this IDTA

- 6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' intention to provide the Appropriate Safeguards.
- 6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the meaning which is most consistent with UK Data Protection Laws applies.
- 6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which mostly closely aligns with the UK Data Protection Laws applies.
- 6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits either Party's liability to Relevant Individuals or to the ICO under this IDTA or under UK Data Protection Laws.
- 6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit any liability to Relevant Individuals or to the ICO, then that wording will not apply.
- 6.6 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):
- 6.6.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Individual's rights, in which case those terms will override the IDTA; and

- 6.6.2 the inconsistent or conflicting terms of the Linked Agreement are expressly required by Article 28 UK GDPR, in which case those terms will override the IDTA.
- 6.7 The words “include”, “includes”, “including”, “in particular” are used to set out examples and not to set out a finite list.
- 6.8 References to:
  - 6.8.1 singular or plural words or people, also includes the plural or singular of those words or people;
  - 6.8.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and
  - 6.8.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

## **7. Which laws apply to this IDTA**

- 7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales.

## **How this IDTA provides Appropriate Safeguards**

### **8. The Appropriate Safeguards**

- 8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:
  - 8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and
  - 8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Individuals of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.
- 8.2 The Exporter promises that:
  - 8.2.1 this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards, and it can demonstrate this (which may be by having carried out a TRA); and

8.2.2 if the Importer reasonably requests it will provide it with a copy of any TRA.

8.3 The Importer promises that:

- 8.3.1 prior to entering into this IDTA it has provided the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA (the "Importer Information");
- 8.3.2 the Importer Information is complete and accurate;
- 8.3.3 it is not aware of any Local Laws which contradict its obligations in this IDTA and it has taken reasonable steps to verify this;
- 8.3.4 it will co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;
- 8.3.5 it will review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and
- 8.3.6 it will inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 Each Party promises that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Individuals of such a Personal Data Breach.

## **9. Reviews to ensure the Appropriate Safeguards continue**

9.1 Each Party agrees to:

- 9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and
- 9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

- 9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:
  - 9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed;
  - 9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and
  - 9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

## **10. The ICO**

- 10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.
- 10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
- 10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

## **The Exporter**

### **11. Exporter's obligations**

- 11.1 The Exporter agrees that:
  - 11.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer;
  - 11.1.2 it has and will comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;
  - 11.1.3 it has and will comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and
  - 11.1.4 it has carried out reasonable checks on the Importer and on that basis considers that the Importer is able to comply with this IDTA.
- 11.2 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

- 11.3 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Individuals or any Third Party Controller. The Exporter may pass these on via a third party if it is reasonable to do so.
- 11.4 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Individuals under Local Law and this IDTA.

## **The Importer**

### **12. General Importer obligations**

- 12.1 The Importer must:
  - 12.1.1 only Process the Transferred Data for the Purpose;
  - 12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;
  - 12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;
  - 12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;
  - 12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and
  - 12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).
- 12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

### **13. Importer's obligations if it is subject to UK Data Protection Laws**

- 13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:
  - 13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- **Section 14** (Importer's obligations to comply with key data protection principles);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 20** (How Relevant Individuals can exercise their data subject rights); and
- **Section 21** (How Relevant Individuals can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

#### **14. Importer's obligations to comply with key data protection principles**

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that each Relevant Individual is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients of the Transferred Data;

The Importer can comply with this Section 14.2.1 if the information is given (or has already been given) to the Relevant Individuals by the Exporter or another party.

The Importer does not need to comply with this Section 14.2.1 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available;

14.2.2 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.3 ensure that the Transferred Data Processed by the Importer is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correcting or deleting any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.4 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

## 15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

- 15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Individuals, stop it from continuing, and prevent it happening again; and
- 15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Individuals of such a Personal Data Breach.

15.2 If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller.

15.3 If the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Individual the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

- 15.3.1 a description of the nature of the Importer Personal Data Breach;
- 15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
- 15.3.3 likely consequences of the Importer Personal Data Breach;
- 15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Individuals, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place; and
- 15.3.5 contact point for more information.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay. The Importer will provide any other information reasonably requested by the Exporter.

15.4 If the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Individual:

- 15.4.1 if the Importer is a Processor or Sub-Processor: assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform the ICO, any other relevant regulator or

authority and Relevant Individuals about the Importer Personal Data Breach Without Undue Delay; or

- 15.4.2 if the Importer is a Controller: inform those Relevant Individuals Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Individuals are informed in an equally effective manner;

- 15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach it (including to minimise the harmful effects on Relevant Individuals, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Individuals of such a Personal Data Breach.

## **16. Transferring on the Transferred Data**

- 16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, and it is for the Purpose, does not breach the Linked Agreement, and one of the following apply:

- 16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA, and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or
- 16.1.2 the third party has been added to this IDTA as a Party; or
- 16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or
- 16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or
- 16.1.5 it is to the UK or an Adequate Country.

- 16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

## **17. Importer's responsibility if it authorises others to perform its obligations**

- 17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16). If the Importer is the Exporter's Processor or Sub-Processor it must also comply with the Linked Agreement or be with the written consent of the Exporter.
- 17.2 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor must only Process the Transferred Data on its instructions.
- 17.3 The Importer remains fully liable to the Exporter, the ICO and Relevant Individuals for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or agent to perform them.

## **What rights do individuals have?**

### **18. The right to a copy of the IDTA**

- 18.1 If a Party receives a request from a Relevant Individual for a copy of this IDTA:
  - 18.1.1 it will provide the IDTA to the Relevant Individual and inform the other Party, as soon as reasonably possible;
  - 18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;
  - 18.1.3 it may redact information in the Tables if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Individual with a summary of those redactions so that the Relevant Individual can understand the content of the Tables.

### **19. The Importer's contact details for the Relevant Individuals**

- 19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.
- 19.2 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.
- 19.3 The Importer must make sure those contact details are always easy to access for all Relevant Individuals and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

## **20. How Relevant Individuals can exercise their data subject rights**

- 20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.
- 20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.
- 20.3 The following Sections of this Section 20, relate to a Relevant Individual's Personal Data which forms part of the Transferred Data the Importer is Processing.
- 20.4 If the Relevant Individual requests, the Importer must provide them with a copy of their Transferred Data:
  - 20.4.1 Without Undue Delay (and in any event within one month);
  - 20.4.2 free of charge;
  - 20.4.3 in plain English that is easy to understand; and
  - 20.4.4 in an easily accessible form,  
together with:
  - 20.4.5 (if needed) a plain language explanation of the Transferred Data so that it is understandable to the Relevant Individual; and
  - 20.4.6 information that the Relevant Individual has the right to bring a claim for compensation under this IDTA.
- 20.5 If a Relevant Individual requests, the Importer must:
  - 20.5.1 rectify inaccurate or incomplete Transferred Data;
  - 20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;
  - 20.5.3 cease using it for direct marketing purposes; and
  - 20.5.4 comply with any other reasonable request of the Relevant Individual.
- 20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Individual based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Individual or similarly significantly affects them, except if it is permitted by Local Law and:
  - 20.6.1 the Relevant Individual has given their explicit consent to such; Decision-Making; or

- 20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Individuals in relation to such Decision-Making, as to the relevant protection the Relevant Individual would have if such Decision-Making was in the UK; or
- 20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Individuals in relation to such Decision-Making, as to the relevant protection the Relevant Individual would have if such Decision-Making was in the UK.

## **21. How Relevant Individuals can exercise their data subject rights – if the Importer is the Exporter’s Processor or Sub-Processor**

- 21.1 Where the Importer is the Exporter’s Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

## **22. Rights of Relevant Individuals are subject to the exemptions in the UK Data Protection Laws**

- 22.1 The Importer is not required to respond to requests or provide notifications under Sections 18, 19, 20, 21 and 23 if:
  - 22.1.1 it is unable to reasonably verify the identity of an individual making the request; or
  - 22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Individual a reasonable fee; or
  - 22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual’s request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge and that the Relevant Individual is entitled to bring a claim for compensation under this IDTA.

## **How to give third parties access to Transferred Data under Local Laws**

### **23. Access requests and direct access**

- 23.1 In this Section 23 an “Access Request” is a legally binding request to access any Transferred Data and “Direct Access” means direct access to any Transferred Data by public authorities of which the Importer is aware.

- 23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.
- 23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Individuals.
- 23.4 In so far as Local Laws allow, the Importer must:
  - 23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/Accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and
  - 23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

## **24. Giving notice**

- 24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.
- 24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.
- 24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

## **25. General clauses**

- 25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:
  - 25.1.1 contain all the terms and conditions agreed by the Parties; and
  - 25.1.2 override all previous contacts and arrangements, whether oral or in writing.

- 25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.
- 25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party.
- 25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.
- 25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
- 25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.
- 25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.
- 25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:
  - 25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;
  - 25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and
  - 25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

## **What happens if there is a breach of this IDTA?**

### **26. Breaches of this IDTA**

- 26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:
  - 26.1.1 has breached this IDTA; or

- 26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.
- 26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Individual or the other Party.

## **27. Breaches of this IDTA by the Importer**

- 27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 27.2 Until there is no ongoing Significant Harmful Impact on Relevant Individuals:
- 27.2.1 the Exporter must suspend sending Transferred Data to the Importer;
- 27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and
- 27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Individual when it is Processed by or on behalf of that third party receiver:
- 27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and
- 27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor, make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).
- 27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Individuals, the Exporter must end this IDTA under Section 30.1.

## **28. Breaches of this IDTA by the Exporter**

- 28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.
- 28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Individuals, the Exporter must suspend sending Transferred Data to the Importer.
- 28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Individuals, the Importer must end this IDTA under Section 30.1.

## **Ending the IDTA**

### **29. How to end this IDTA without there being a breach**

- 29.1 Except where Section 29.2 applies the IDTA will end at:
  - 29.1.1 the end of the Term stated in Table 2: Transfer Details; or
  - 29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other, at the end of the notice period stated.
- 29.2 When the events in Section 29.1 occur, if the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then:
  - 29.2.1 it will notify the Exporter Without Undue Delay;
  - 29.2.2 it will retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and
  - 29.2.3 it will stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end.

### **30. How to end this IDTA if there is a breach**

- 30.1 A Party may end this IDTA immediately by giving the other Party written notice if:
  - 30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and:

- 30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or
- 30.1.1.2 the breach and its significant harmful impact cannot be corrected;
- 30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

### **31. What must the Parties do when the IDTA ends?**

31.1 When this IDTA ends (no matter what the reason is):

- 31.1.1 the Exporter must stop sending Transferred Data to the Importer;
- 31.1.2 if the Importer is the Exporter's Processor or Sub-Processor: delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;
- 31.1.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.
- 31.1.4 the following provisions will continue in force after this IDTA ends (no matter what the reason) :
  - **Section 1** (This IDTA and Linked Agreements);
  - **Section 2** (Legal Meaning of Words);
  - **Section 6** (Understanding this IDTA);
  - **Section 7** (Which laws apply to this IDTA);
  - **Section 10** (The ICO);
  - **Sections 11.1 and 11.3** (Exporter's obligations);
  - **Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6** (General Importer obligations);
  - **Section 13.1** (Importer's obligations if it is subject to UK Data Protection Laws);
  - **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
  - **Section 24** (Giving notice);

- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Individuals and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration);
- **Section 36** (IDTA Arbitration Scheme Rules); and
- **Section 37** (Legal Glossary).

## How to bring a legal claim under this IDTA

### 32. Your liability

- 32.1 The Parties remain fully liable to Relevant Individuals for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.
- 32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Individuals for the entire damage suffered by the Relevant Individual, caused directly or indirectly by:
- 32.2.1 Party One's breach of this IDTA; and/or
  - 32.2.2 a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal) unless Party One can prove it is not in any way responsible for the event giving rise to the damage.
- 32.3 If one Party has paid compensation to a Relevant Individual under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.
- 32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

### 33. How Relevant Individuals and the ICO may bring legal claims

33.1 The Relevant Individuals are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Individuals);
- **Section 20** (How Relevant Individuals can exercise their data subject rights);
- **Section 21** (How Relevant Individuals can exercise their data subject rights- if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);

- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends; and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Individuals.

- 33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1.1 and 11.1.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).
- 33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).
- 33.4 The Parties do not need the consent of any Relevant Individual or the ICO to make changes to this IDTA.
- 33.5 In bringing a claim under this IDTA, a Relevant Individual may be represented by a not-for profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

#### **34. Courts legal claims can be brought in**

- 34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).
- 34.2 The Exporter may bring a claim against the Importer in connection with this IDTA in any court in any country (including non-contractual claims).
- 34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
- 34.4 Relevant Individuals and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country.
- 34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Individual or the ICO in connection with the Transferred Data (including claims in arbitration).

## 35. Arbitration

- 35.1 Instead of bringing a claim in court, any Party, a Relevant Individual or the ICO may bring a claim for breach in arbitration under the IDTA Arbitration Scheme Rules.
- 35.2 The IDTA Arbitration Scheme Rules are incorporated into this IDTA. Any claim in arbitration under this IDTA may also consider questions regarding the existence, validity or termination of the IDTA entered into by the Parties.

## 36. IDTA Arbitration Scheme Rules

[The ICO is considering the introduction of arbitration as an optional dispute resolution mechanism under the IDTA.

The IDTA Arbitration Scheme would be an optional dispute resolution mechanism for claims brought by:

- the parties to an IDTA;
- the data subjects in relation to data transferred under an IDTA; and
- the ICO itself.

The ICO's objective is to offer the option of arbitration, which may sometimes be quicker, easier and more affordable than enforcement via the courts. The adoption of any scheme will be subject to these objectives being achievable.

If adopted, the final IDTA would include an arbitration clause requiring the parties to submit to arbitration under specified rules, with a UK seat of arbitration.]

## 37. Legal Glossary

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)	Guidance (this is not part of the IDTA)
Access Request	As defined in Section 23.1, as a legally binding request to access any Transferred Data.	A person or organisation (which is not a party to the IDTA) may make a legally binding request for a copy of any Transferred Data or for access to the Transferred Data. This could be by a private company or public authority, such as national security or law enforcement agency.

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
		<p>The form this will take will depend on Local Law. For example, it could be a Court order, a warrant or a subpoena.</p> <p>You should have considered this as part of any TRA. You can review our TRA Tool for further guidance.</p> <p>For or the IDTA to maintain Appropriate Safeguards, you will have decided that:</p> <ul style="list-style-type: none"> <li>• the Local Laws which govern Access Requests are sufficiently similar to UK laws;</li> <li>• the risk of this type of Access Request is minimal; or</li> <li>• if an Access Request is made the risk of harm to the Relevant Individuals is low.</li> </ul>
Adequate Country	<p>A third country, or:</p> <ul style="list-style-type: none"> <li>• a territory;</li> <li>• one or more sections within a third country;</li> <li>• an international organisation;</li> </ul> <p>which the Secretary of State has specified by regulations that it provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.</p>	<p>UK “adequacy regulations” set out in law that the legal framework in that country, has been assessed as providing ‘adequate’ protection for individuals’ rights and freedoms for their personal data.</p> <p>The UK has “adequacy regulations” in relation to the following countries and territories:</p> <ul style="list-style-type: none"> <li>• the European Economic Area (EEA) countries;</li> <li>• EU or EEA institutions, bodies, offices or agencies;</li> <li>• Gibraltar;</li> <li>• countries covered by a full EU adequacy decision: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay; and</li> <li>• countries covered by an EU partial finding of adequacy: <ul style="list-style-type: none"> <li>◦ Japan – only covers private sector organisations.</li> </ul> </li> </ul>

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
		<ul style="list-style-type: none"> <li>○ Canada – only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA.</li> </ul>
agreement	No legal definition.	Another word for a written contract which is binding and enforceable.
Appropriate Safeguards	<p>The standard of protection over the Transferred Data and of the Relevant Individual's rights, which is required by UK Data Protection Laws when you are making a restricted transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.</p>	<p>This is the level of protection which the UK GDPR requires must be maintained over the Transferred Data when it passes to the Importer. The protections over the Transferred Data and the Relevant Individual's rights must be sufficiently similar to the relevant protection in the UK.</p> <p>This standard will be met if (other than trivial breaches):</p> <ul style="list-style-type: none"> <li>• The Exporter can comply with the IDTA (including the Security Requirements and Extra Protection Clauses)</li> <li>• The Security Requirements and relevant Extra Protection Clauses are sufficient to prevent the Transferred Data being accidentally or deliberately compromised. You can review our ICO guidance on Security to help you decide on the appropriate level of security.</li> <li>• You are satisfied that the the IDTA with the Extra Protection Clauses provides Appropriate Safeguards and have documented this in a TRA.</li> </ul>
Approved IDTA	The template IDTA laid before Parliament and approved by the ICO in accordance with s117A of the Data Protection Act 2018.	This is the full, approved IDTA with all relevant clauses. It will apply if you if you have made an incorrect selection in the Tables, for example

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
		you have selected you are a Processor when you are a Controller, or you have made a mistake when amending the IDTA or chosen the wrong ICO guidance IDTA.
Article 28 UK GDPR	No legal definition.	Article 28 sets out a list of contract terms that you must include in a contract between a Controller and a Processor.  You can find more information on these obligations in our detailed guidance <a href="#">Contracts and liabilities between controllers and processors</a>
Commercial Clauses	The commercial clauses set out in Part three.	These are the commercial clauses which you and the Importer agree to add to the IDTA.
Controller	As defined in the UK GDPR.	Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.
Damage	All material and non-material loss and damage.	This includes damage and distress.
Data Subject	As defined in the UK GDPR.	The identified or identifiable living individual to whom personal data relates.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Individuals based solely on automated processing, including profiling, using the Transferred Data.	This definition is only used in Section 20.6, so that it is easier to read.

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
Direct Access	As defined in Section 23.1 as direct access to any Transferred Data by public authorities of which the Importer is aware.	<p>This is where public authorities, such as national security or law enforcement agencies use their surveillance powers to directly access the data.</p> <p>You should have considered this as part of any TRA. You can review our TRA Tool for guidance.</p> <p>For the IDTA to maintain Appropriate Safeguards, you will have decided that:</p> <ul style="list-style-type: none"> <li>• the Local Laws which govern Direct Access are sufficiently similar to UK laws;</li> <li>• the risk of this type of Direct Access is minimal; or</li> <li>• if Direct Access does occur the risk of harm to the Relevant Individuals is low.</li> </ul>
Exporter	The exporter identified in Table 1.	You, the Party making the restricted transfer and sending the Transferred Data to the Importer.
Exporter's Processor or Sub-Processor	No legal definition.	Where the Importer is acting on the instructions of the Exporter, as its Processor or Sub-Processor
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.	Having carried out a TRA, these are the clauses you added to provide extra protections to ensure the Appropriate Safeguards. You can review our TRA Tool for guidance.
FAQs	No legal definition.	The FAQs set out in Chapter four, but which do not form part of this IDTA
ICO	The Information Commissioner.	Parliament appoints the Information Commissioner to regulate UK Data Protection Laws.

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
		They are a corporation sole with staff who work to their direction. This is why they are often referred to as the ICO or the Information Commissioner's Office.
IDTA	<p>This agreement (the International Data Transfer Agreement), which is formed by:</p> <p>Part one: Tables</p> <p>Part two: Extra Protection Clauses;</p> <p>Part three: Commercial Clauses; and</p> <p>Part four: Mandatory Clauses.</p>	<p>This contract, which includes the standard contractual clauses published by the Information Commissioner, as an appropriate safeguard for restricted transfers, under Article 46 UK GDPR.</p> <p>UK Data Protection Laws require that for the IDTA to provide Appropriate Safeguards you must carry out a TRA, and you may need to include Extra Protection Clauses.</p> <p>You can review our TRA Tool for guidance.</p>
IDTA Arbitration Scheme Rules	The rules set out in Section 36 which apply when a Party, a Relevant Individual or the ICO bring a claim under or in relation to this IDTA in Arbitration.	Because arbitration is outside of the Court system and rules, you need to set your own rules as to how the process will work. This is done for you in the IDTA.
Importer	The importer identified in Table 1: Parties & Signature.	The Party receiving the Transferred Data from you.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.	A contact point, including email address, of an individual with whom Data Subjects may make requests and complaints, whose contact details must always be reasonably easy to access by all Data Subjects.
Importer Information	As defined in Section 8.3.1 as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer,	The Importer has to provide the Exporter with information about Local Laws and any other information which may affect the Appropriate Safeguards, and has to

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
	including for the Exporter to carry out any TRA.	<p>confirm that this information is accurate.</p> <p>This information needs to be provided before the parties enter into the IDTA, so the Exporter can carry out its TRA, and the Importer need to do regular checks to make sure the Importer Information remains accurate and complete. These updates must be at least as frequently as the Review Dates.</p>
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.	<p>A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.</p> <p>In short, it is a personal data breach whenever any personal data is:</p> <ul style="list-style-type: none"> <li>• accidentally lost, destroyed, corrupted or disclosed;</li> <li>• accessed by someone, or someone passes it on, without proper authorisation; or</li> <li>• made unavailable and this unavailability has a significant negative effect on individuals.</li> </ul>
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).	These are any other contracts between the Exporter and Importer which relate to the Processing of the Transferred Data, or relate to products or services which involve the Transferred Data.
Local Laws	Laws which are not the laws of the UK and which bind the Importer.	These are the laws in any country other than the UK, where the Importer is based or the Transferred Data is located.

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.	
Notice Period	As set out in Table 2: Transfer Details.	<p>If you or the Importer wish to end the IDTA you can do so by sending the other a written notice. The Notice Period starts when this notice is received by the other Party. And the IDTA will end after the Notice Period has finished.</p> <p>This applies where one of the Parties ends the IDTA and this is not because (i) they have provided that the other Party was at fault; or (ii) the Appropriate Safeguards have been reduced.</p>
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.	These are the Exporter and the Importer.
Personal Data	As defined in the UK GDPR.	<p>Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as:</p> <ul style="list-style-type: none"> <li>• a name;</li> <li>• an identification number;</li> <li>• location data;</li> <li>• an online identifier; or</li> <li>• one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.</li> </ul>
Personal Data Breach	As defined in the UK GDPR.	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
Processing	<p>As defined in the UK GDPR.</p> <p>When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.</p>	<p>Almost anything you do with data counts as processing, including:</p> <ul style="list-style-type: none"> <li>• collecting;</li> <li>• recording;</li> <li>• storing;</li> <li>• using;</li> <li>• analysing;</li> <li>• combining;</li> <li>• disclosing; or</li> <li>• deleting.</li> </ul>
Processor	As defined in the UK GDPR.	A person, public authority, agency or other body which processes personal data on behalf of a Controller.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.	<p>The purposes for which the Importer is allowed to use the Transferred Data.</p> <p>This is the reason why you are sending the Transferred Data to the Importer, so that it can use the Transferred Data for these purposes.</p>
Redact	No legal definition.	To edit a document to remove or black out information which you should not disclose.
Relevant Individual	A Data Subject of the Transferred Data.	These are the individuals whose Personal Data you send to the Importer.
restricted transfer	No legal definition.	An international transfer of Personal Data which is restricted under Article 44 UK GDPR, and can only be made if the Exporter complies with Chapter V UK GDPR.

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
Review Dates	The review dates or period for the review of the IDTA as set out in Table 2: Transfer Details .	<p>These review dates are important as they are when you will be checking whether the IDTA continues to provide the Appropriate Safeguards.</p> <p>The Importer must check and update the Importer Information, and the Exporter must review its TRA, Extra Protection Clauses and the Security Requirements.</p>
Section	No legal definition.	A numbered section of the IDTA
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Individual or the other Party.	<p>Something which reduces the level of protection in the IDTA in a way which is not trivial.</p> <p>For example, because it reduces the protection over the Transferred Data or puts the Data Subjects at a higher risk.</p> <p>This may be because the level of technical or organisational security is lower than required by the IDTA or because a Local Law means the Importer cannot comply with the IDTA.</p>
Special Category Data	As described in the UK GDPR.	<p>Personal data revealing:</p> <ul style="list-style-type: none"> <li>• racial or ethnic origin;</li> <li>• political opinions;</li> <li>• religious or philosophical beliefs;</li> <li>• trade union membership;</li> <li>• the processing of genetic data;</li> <li>• biometric data for the purpose of uniquely identifying a natural person;</li> <li>• health; or</li> <li>• a natural person's sex life or sexual orientation.</li> </ul>

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
Start Date	As set out in Table 1: Parties and signature.	The date the IDTA takes effect from.  If you and the Importer agree, this date can be before or after the date you both sign the IDTA.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf.  This includes Sub-Processors of any level, for example a Sub-Sub-Processor.	A Sub-Processor is where the Processor has sub contracted some or all of its obligations as a Processor.  There may be long chains of Processors and Sub-Processors, going to many layers of Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.	
Term	As set out in Table 2: Transfer Details.	
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor  If there is not a Third Party Controller this can be disregarded.	For some restricted transfers, the Exporter will be a Processor and its Controller is a third party, ie not the Importer.  In that case, there are times when the Exporter's Controller needs to be informed or involved.  If there is no Third Party Controller, then the words should stay in the IDTA (as you cannot amend it) but they would be disregarded by a Court or Arbitrator.
TRA or Transfer Risk Assessment	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards	Before using an IDTA for a restricted transfer, you must carry out a transfer risk assessment to make sure that the IDTA provides the Appropriate Safeguards, taking into consideration the circumstances of the restricted

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)	Guidance (this is not part of the IDTA)
		transfer, including the laws and practices of the destination country. The ICO has published a TRA Tool to help you to do this.
transfer	No legal definition	This is where one legal entity authorises or allows a separate legal entity (itself or using its Processor or Sub-Processor) to Process data.
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details	This is the Personal Data you are sending to the Importer.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.	The main legislation is UK GDPR and Data Protection Act 2018. This will also cover e-Privacy legislation and the tort of privacy. The scope of UK Data Protection Laws will change over time, as laws are updated and Courts make decisions how to interpret the law.
UK GDPR	The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4)).	
Without Undue Delay	Without undue delay, as that phrase is interpreted in the UK GDPR.	Any delay must not be excessive and must be proportionate to the impact on the relevant persons or organisations involved. If you are considering whether a delay is proportionate or not, you can take into account the seriousness of the relevant issue and the impact on Data Subjects,

<b>Word or Phrase</b>	<b>Legal definition</b> <b>(this is how this word or phrase must be interpreted in the IDTA)</b>	<b>Guidance</b> <b>(this is not part of the IDTA)</b>
		<p>the Importer, Exporter and Third Party Controller (if any).</p> <p>This means that the more serious the impact on a person or organisation, such as a Data Subject, the shorter the delay may be. But if the impact is not serious, the delay can be longer.</p>
written record of its Processing	No legal definition.	<p>There is no set format for written records, but they should be kept in a manner which is capable of being shared with the Exporter and the ICO if necessary.</p> <p>Controllers and Processors who are subject to the UK GDPR are required to maintain a written record under Article 30 UK GDPR, and so it may be helpful to refer to those requirements</p>

## Chapter 4: Frequently Asked Questions

---

### How do I complete Table 1: Parties and Signature?

#### **The Start Date:**

The Start Date should be on or before the first date that you intend to transfer the Transferred Data. If both parties agree, it can be before or after you both sign.

#### **Who is the Exporter?**

The Exporter is the organisation (or person) that is subject to the UK GDPR and is sending the Transferred Data to a separate legal entity that is not in the UK.

You must include full details, including the corporate address and company number or other corporate identification number. This is so the legal entity can be clearly identified in future years. For example, companies can change names so you need to be able to pinpoint which company it is.

#### **Who is the Importer?**

The Importer is the organisation (or person) receiving or accessing the Transferred Data that is outside of the UK.

You must include full details, including the corporate address and company number or other corporate identification number. This is so the legal entity can be clearly identified in future years. For example, companies can change names so you need to be able to pinpoint which company it is.

#### **Who should the Key Contact be?**

This is the person at the Importer or Exporter who needs to receive any important communications or notices from the other Party.

You can update this information by giving 14 days written notice to the other Party. For example, sending an email to the Key Contact of the other Party.

#### **Who should the Importer Data Subject Contact be?**

These are the contact details which individuals can use to contact the Importer about their Personal Data.

It does not need to be a named person, but someone needs to receive these calls and emails and be available to speak or communicate with the individuals during normal UK working hours.

For example, it could be:

- an email address: [complaints@importer.biz](mailto:complaints@importer.biz); and
- a telephone number (which is not charged at a premium): Complaints: 123 456789

In addition, you may also have a postal address:

- Importer Complaints, 123 Restricted Transfer Road, Overseas 456.

But you should not just have a postal address.

### **How do we sign the IDTA?**

You can sign the IDTA in Table 1. This makes it clear that the IDTA is a binding contract.

The IDTA should be signed by someone who has the authority to enter a contract on behalf of each Party.

The signature may be a normal signature (or “wet ink” signature), an electronic signature using a secure electronic signature, or a typed digital signature if you intend this to be a signature.

It is possible that the IDTA may be binding if you do not sign the document but you make it clear that you have agreed to its terms, for example by sending an email which states this. However it is more certain and clear if both Parties sign.

You can choose to:

- both sign one IDTA (and each keep a copy);
- both sign two identical IDTAs (and each keep one); or
- each sign one IDTA and then swap, so you each have an identical copy with the other’s signature.

Once you have both signed the IDTA, if you do not comply with its terms, the other Party, Relevant Individuals [or the ICO] can take action to enforce its terms and claim compensation.

### **How do I complete Table 2: Transfer Details?**

#### **How do I choose which UK country’s law should apply to the IDTA?**

You would normally choose the law of the UK country in which you are based.

#### **How do I choose which UK country’s courts claims can be made in?**

You would normally choose the court of the UK country in which you are based.

## **How do I know what the relationship is between the Parties? <sup>9</sup>**

It can be difficult to decide whether you and the Importer are Controllers or Processors (or Sub-Processors), and whether or not UK GDPR applies to the Importer.

A good place to start is our guidance on Controllers and Processors.

If you are still not sure, you should consider seeking professional advice, as it is important that you choose the right option, as the obligations are different.

## **How do I know if UK GDPR applies to the Importer? <sup>10</sup>**

The UK GDPR will apply to the Importer if:

- it is offering goods or services to individuals in the UK;
- it is monitoring the behaviour of individuals located in the UK; or
- its processing of the Transferred Data is in the context of a UK establishment, which may be an establishment of a separate organisation.

If you are still not sure, you should consider seeking professional advice, as it is important that you choose the right option, as the obligations will be different.

## **What is a Linked Agreement? <sup>11</sup>**

The IDTA only covers the restricted transfer of the Transferred Data. It does not cover other aspects of the relationship between you and the Importer. It will be unusual for the IDTA to be entered into on its own.

You may have a service agreement or data sharing agreement between you and the Importer. If the Importer is your Processor or Sub-Processor you are required by Article 28 UK GDPR to have a contract in place containing specific terms.

These 'Linked Agreements' are useful as they often contain a lot of the information you need to complete the Tables. In that case you can just refer to the relevant section of the Linked Agreement.

---

<sup>9</sup> This section may need to be updated following the Consultation Section 1: Proposal and plans for the ICO to update its guidance on international transfers

<sup>10</sup> This section may need to be updated following the Consultation Section 1: Proposal and plans for the ICO to update its guidance on international transfers

<sup>11</sup> This section may need to be updated following the Consultation Section 1: Proposal and plans for the ICO to update its guidance on international transfers

## Should I allow changes to the Linked Agreement to automatically apply to the IDTA?

This really depends on the circumstances of your transfer. The benefit is that it keeps the IDTA aligned with the Linked Agreement.

It is not a good idea if you are concerned that changes to the Linked Agreement might go through without anyone reviewing the impact on the IDTA and TRA.

A better alternative might be to link the terms of the Linked Agreement to the IDTA, so that the IDTA is formally updated and the Linked Agreement automatically changes to match it.

## What is the Term?

This is the time period when the IDTA is in force.

As a minimum it should be the time period while the Importer is Processing the Transferred Data. If it turns out the time period is too short, you and the Importer can always agree to extend the term. (See How do I make changes to the IDTA?)

You have the choice to:

- Give a specific Term. For example, 1 month or 2 years.
- Connect the term to the Linked Agreement, so they run in parallel.
- Only if the Importer is a Controller, allow the Term to continue indefinitely so long as the Importer still needs to Process the Transferred Data for the Purpose which you specify (further down in this Table).

## How do I decide on the Notice period to end the IDTA?

If you have a Linked Agreement, you may want this Notice period to be identical to the one in the Linked Agreement.

If not, you should think about what is a reasonable period for you and the Importer to amicably make arrangements for the IDTA to end and (if relevant) for you or they to make alternative arrangements with a third party.

For example, if the importer sends out your marketing emails, how long would it take you both to arrange for that service to end and all the information be returned or destroyed, and for you to find an alternative supplier.

For smaller contracts a notice period of 1 to 3 months might be appropriate. For major contracts it can be up to 1 year.

If you agree a notice period which is too long, the courts might decide this is unreasonable and replace it with a shorter one.

## **Why do we have restrictions on the Importer forwarding the data?**

These restrictions are very important for the Appropriate Safeguards. Without them the Transferred Data would lose the IDTA's protection if the Importer simply forwarded the data to another organisation.

## **How do I decide which restrictions on transferring the data on to someone else are right for my IDTA?**

There are a number of options, and you need to read them carefully to consider which is most suitable. There are specific restrictions and also general restrictions which refer to Section 16.

Check your Linked Agreement, as there may already be restrictions in there.

Check your TRA, you may have identified a particular risk in forwarding the data.

In general, if there is no need for the Importer to transfer on the data, then you should not allow it to. Tick "No specific restrictions" and "The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16".

If in doubt, choose a selection which provides more restrictions than not. You can always agree to change this later (See How do I make changes to the IDTA?).

## **How often should I review the IDTA?**

At least once a year, and more often if the data is very high risk. This review must include your TRA.

If nothing has changed, then the review will be very straightforward. But it's still important to check that nothing has changed.

## **How do I complete Table 3: Transferred Data?**

You should have already collected together all this information when you did your TRA, so you should have this information to hand.

All the information about the Transferred Data may be set out in a Linked Agreement, and you can just insert here the reference to that.

There is also an option so that when you update the Linked Agreement, it automatically updates the IDTA. Think carefully before choosing this option, it can be helpful if you are certain that you will *always* want those changes to apply to the IDTA.

Do consider whether it is easy enough to repeat that information in this Table so that a Data Subject can understand the intended processing without seeing the Linked Agreement.

### **What do I include in the Transferred Data?**

You should include details of the categories of Personal Data, Special Category Data and Criminal Offences Data that are to be transferred

You should include all categories of Data Subjects. **Do not include the names of Data Subjects.**

For routine transfers, you might find this checklist helpful:

Each category includes current, past and prospective data subjects. Where any of the following is itself a business or organisation, it includes their staff.

- staff including volunteers, agents, temporary and casual workers
- customers and clients (including their staff)
- suppliers (including their staff)
- members or supporters
- shareholders
- relatives, guardians and associates of the data subject
- complainants, correspondents and enquirers;
- experts and witnesses
- advisers, consultants and other professional experts
- patients
- students and pupils
- offenders and suspected offenders
- other (please provide details of other categories of data subjects):

### **What is the Purpose?**

These are the purposes for which the Importer is allowed to use the Transferred Data.

This is the reason why you are sending the Transferred Data to the Importer, so that it can use the Transferred Data for these purposes.

The sentence at the bottom is important “And any other purposes which are compatible with the purposes set out above”. This flexibility is permitted under UK GDPR. It helps the Importer to use the Transferred Data for peripheral purposes, and if you had thought about it when you entered this IDTA, you would agree should be covered.

## How do we complete Table 4: Security Requirements?

The higher risk to the rights of individuals of the Transferred Data, the more detail is needed here. You may even need help from an information security specialist.

For restricted transfers which do not cause a particularly high risk to the rights of individuals, you can use the checklist below. For example, where the personal data transferred is:

- not special category data;
- not criminal convictions and offences data;
- not personal details issued as an identifier by a public authority;
- not bank account, credit card or other payment data; and
- not a large volume of data.

### Security Requirements Checklist:

Consider each statement, and the relevant guidance set out below.

Tick the box next to those statements which apply, and add supplementary notes to provide any further relevant detail of those security measures.

Your security requirements will always depend upon your particular circumstances. Further guidance which may be of assistance:

- A Practical Guide to IT Security
- Cyber Security: Small Business Guide
- Cyber Essentials Scheme

**We use firewalls to protect our internet connection** This will be your first line of defence against an intrusion from the internet.

Supplementary details of firewalls used (add any relevant details):

**We choose the most appropriate secure settings for our devices and software** Most hardware and software will need some level of set-up and configuration in order to provide effective protection.

Supplementary details of security settings used (add any relevant details):

- We control who has access to your data and services** Restrict access to your system to users and sources you trust.

Supplementary details of how access to your system is controlled (add any relevant details):

- We protect ourselves from viruses and other malware?** Anti-virus products can regularly scan your network to prevent or detect threats.

Supplementary details of antivirus and malware protection used (add any relevant details):

- We keep our software and devices up-to-date** Hardware and software needs regular updates to fix bugs and security vulnerabilities.

Supplementary details of how software and devices are kept up to date (add any relevant details, including details of the software packages, cloud services and devices you use in processing the personal data transferred, and how you keep those updated):

- We regularly backup our data** Regular backups of your most important data will ensure it can be quickly restored in the event of disaster or ransomware infection.

Supplementary details of how data is backed up (add any relevant details):

## How do we complete Part two: Extra Protection Clauses?

### **Do I need to do a Transfer Risk Assessment for every restricted transfer?**

Yes. UK Data Protection Laws currently require that a transfer risk assessment must be carried out prior to you using the IDTA to make a restricted transfer.

We have a Transfer Risk Assessment Tool, which may be helpful.

### **How do I decide on the Extra Protection Clauses?**

For routine transfer, the TRA Tool will guide you through, and suggest some extra steps and protections you can take, including Extra Protection Clauses.

If your transfer is high risk or complex, you may need to seek professional advice, which can also help you complete this section.

## How do we complete Part three: Commercial Clauses?

### **Do I need to include any commercial clauses?**

No. It is optional. And if you have a Linked Agreement it is probably unnecessary as the commercial parts of your agreement can be recorded there.

Be cautious when adding Commercial Clauses, because if you inadvertently reduce the level of protection of the IDTA, then your restricted transfer may be in breach of UK GDPR. You may want to seek professional advice.

[See Chapter 5 for some optional commercial clauses you might want to use]

## Understanding the Mandatory Clauses

### **What are “Appropriate Safeguards” and why is this so important in the IDTA?**

This is the standard of protection which the UK GDPR requires must be maintained over the Transferred Data when it passes to the Importer using an IDTA. To comply with UK GDPR the IDTA must maintain this standard.

Under UK Data Protection Laws, you should carry out a Transfer Risk Assessment, or TRA. The purpose of the TRA is for you to check that the IDTA provides the Appropriate Safeguards for the Transferred Data and Relevant Individuals' rights. It has to include giving the Relevant Individuals effective rights which they can enforce.

The Appropriate Safeguards are made up of:

- UK GDPR requirements which apply to one or both parties;
- the contractual obligations in the IDTA;
- how they both operate in the country where the Importer is based;
- how they both can be enforced by the Exporter and Relevant Individuals; and
- how the ICO can investigate and enforce against the Exporter and the Importer.

The baseline for this standard is the UK GDPR and how it operates in the UK. But that does not mean the protections must be identical when Transferred Data goes to an Importer.

First, we can consider which protections are relevant for the particular restricted transfer. For example, if there is no special category or criminal offences data transferring, you don't need to worry about the additional UK GDPR protections for that data.

Second, the standard of protection needs to be **sufficiently similar** to the UK baseline. But how similar is that?

UK GDPR doesn't give individuals absolute protection. It protects data subjects against disproportionate interference with their rights. This means that individuals' protection after a transfer doesn't need to be absolute either: i.e. it doesn't need to be better than UK GDPR.

In making this assessment we can be guided by the Right to Privacy in Article 8 of the European Convention of Human Rights. This sets out a principle of proportionality when balancing the Right to Privacy against the exceptions to that Right (set out in Article 8(2) UK GDPR).

There are no easy or clear answers to this. But we have taken this into account when designing the TRA Tool. This can help you find the right standard of protection, and find the proportionate balance between your interests in making the restricted transfer and the protection needed for the Relevant Individuals, which results in the Appropriate Safeguards.

[Section by Section guidance to be included in final version]

## Chapter 5: Guidance Templates

---

For example, we may include:

- Optional extra protection clauses
- Optional commercial clauses
- A template to make changes to the IDTA
- A multi-party IDTA
- Example of a completed TRA & IDTA